Appendix B
DHFS HIPAA Security Risk Assessment Architecture

			Organizational Security Risk Assessment										Information System Assessment***				Platforms			
			DHFS-wide	DDES Facilities*	DDES Central Office	DHCF	DPH BCDPHP	DCFS BMCW	DMT BIS/BFS	OLC	OSF AA**	OPRA		HSRS	Insight	WiSACWIS		DHFS WAN		
	Administrative Safeguards																			**Administrative Safeguards**
	Security Management Process																			Security Management Process
1		Risk analysis	InHouse										1				1		1	Risk analysis
2		Risk management	InHouse										2				2		2	Risk management
3		Sanction Policy	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	3				3		3	Sanction Policy
4		Information System Activity Review											4	RFP	RFP	RFP	4	RFP	4	Information System Activity Review
5	Assigned Security Responsibility		InHouse										5				5		5	Assigned Security Responsibility
	Workforce Security																			Workforce Security
6		Authorization and/or Supervision	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	6	InHouse	InHouse	InHouse	6	InHouse	6	Authorization and/or Supervision
7		Workforce Clearance Procedure	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	7				7		7	Workforce Clearance Procedure
8		Termination Procedures	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	8				8		8	Termination Procedures
	Information Access Management																			Information Access Management
9		Isolating Health care Clearinghouse Function				InHouse							9				9		9	Isolating Health care Clearinghouse Function
10		Access Authorization	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	10	RFP	RFP	RFP	10	RFP	10	Access Authorization
11		Access Establishment and Modification	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	11	RFP	RFP	RFP	11	RFP	11	Access Establishment and Modification
	Security Awareness and Training																			Security Awareness and Training
12		Security Reminders	InHouse										12				12		12	Security Reminders
13		Protection from Malicious Software	InHouse										13				13		13	Protection from Malicious Software
14		Log-In Monitoring	InHouse										14				14		14	Log-In Monitoring
15		PAssDocword Management	InHouse										15				15		15	PAssDocword Management
	Security Incident Procedures																			Security Incident Procedures
16		Response and Reporting	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	16				16		16	Response and Reporting
	Contingency Plan																			Contingency Plan
17		Data Backup Plan											17				17	InHouse	17	Data Backup Plan
18		Disaster Recovery Plan	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	18	InHouse	InHouse	InHouse	18	InHouse	18	Disaster Recovery Plan
19		Emergency Mode Operation Plan	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	19	InHouse	InHouse	InHouse	19	InHouse	19	Emergency Mode Operation Plan
20		Testing and Revision Procedure	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	20	InHouse	InHouse	InHouse	20	InHouse	20	Testing and Revision Procedure
21		Applications and Dta Criticality Analysis											21				21	InHouse	21	Applications and Dta Criticality Analysis
22	Evaluation		RFP										22				22		22	Evaluation
	BA Contracts and other Arrangements																			BA Contracts and other Arrangements
23		Written Contract or other Arrangement	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	23				23		23	Written Contract or other Arrangement
	Physical Safeguards																			**Physical Safeguards**
	Facility Access Controls																			Facility Access Controls
24		Contingency Operations	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	24				24	InHouse	24	Contingency Operations
25		Facility Security Plan	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	25				25	InHouse	25	Facility Security Plan
26		Access Control and Validation Procedures	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	26				26	InHouse	26	Access Control and Validation Procedures
27		Maintenance Records	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	InHouse	27				27	InHouse	27	Maintenance Records
28	Workstation Use		RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	28				28		28	Workstation Use
29	Workstation Security		RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	29				29		29	Workstation Security
	Device and Media Controls																			Device and Media Controls
31		Disposal	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	31				31		31	Disposal
32		Media Re-Use	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	32				32		32	Media Re-Use
33		Accountability	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	33				33		33	Accountability
34		Data Backup and Storage	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	34				34		34	Data Backup and Storage
	Technical Safeguards																			**Technical Safeguards**
	Access Control																			Access Control
35		Unique User ID											35	InHouse	InHouse	InHouse	35	InHouse	35	Unique User ID
36		Emergency Access Procedure											36	InHouse	InHouse	InHouse	36	InHouse	36	Emergency Access Procedure
37		Automatic Logoff											37	InHouse	InHouse	InHouse	37	InHouse	37	Automatic Logoff
38		Encryption and Decryption											38	InHouse	InHouse	InHouse	38	InHouse	38	Encryption and Decryption
39	Audit Controls		RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	39	RFP	RFP	RFP	39		39	Audit Controls
	Integrity																			Integrity
40		Mechanism to Authenticate E-PHI	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	40	RFP	RFP	RFP	40		40	Mechanism to Authenticate E-PHI
41	Person or Entity Authentication		RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	RFP	41	RFP	RFP	RFP	41		41	Person or Entity Authentication
	Transmission Security																			Transmission Security
42		Integrity Controls											42				42	RFP	42	Integrity Controls
43		Encryption											43				43	RFP	43	Encryption

Areas in gray and items labeled "RFP" are to be assessed by an expert third party. Items labeled "InHouse" will be assessed by DHFS internal audit staff.

Department of Health and Family Services (DHFS-wide) means at the enterprise level

* Division of Disability & Elder Services (DDES) Facilities includes: Central Wisconsin Center (CWC), Northern Wisconsin Center (NWC), Southern Wisconsin Center (SWC), Mendota Mental Health Institute (MMHI), Winnebago Mental Health Institute (WMHI), Wisconsin Resource Center (WRC) and Sand Ridge Secure Treatment Center (SRSTC)

Division of Health Care Financing (DHCF)

Division of Public Health (DPH) Bureau of Chronic Disease Prevention and Health Promotion (BCDPHP)

Division of Children and Family Services (DCFS) Bureau of Milwaukee Child Welfare (BMCW)

Division of Management and Technology (DMT) Bureau of Information Systems (BIS) and Bureau of Fiscal Services (BFS)

Office of Legal Council (OLC)

** Office of Strategic Finance (OSF) Area Administration (AA) includes 5 regional offices: Southern Regional Office (SRO), South Eastern Regional Office (SERO), Northern Regional Office (NRO), North Eastern Regional Office (NERO) and Western Regional Office (WRO)

Office of Program Review and Audit (OPRA)

*** Information System Assessment will also address OMB A-130 requirements for Federally funded systems

Human Services Reporting System (HSRS)

Stockell's Insight Client Server (CS)

Wisconsin Statewide Automated Child Welfare Information System (WiSACWIS)